

located or in association with which the server is to function as a security mechanism. As a parallel to this step of the development of the security system, each of the individualized user access key codes is separately recorded, for example by ganged optical recording machines of the type known to the art for recording information onto CD-ROM disks. Each disk is in the form of an actual physical "CD-ROM key" which is individualized for a particular end user (for example, a customer of a catalog sales organization, a user of a secure database, a customer of a financial institution, etc.).

At this stage of the establishment of the system there is a complete registry of "ultra long" identification key codes stored in a server and there is a distribution of the actual physical CD-ROM disk keys to authorized individual users who are to be provided access to a database.

In order to provide authorized access to an authorized user of the database or "transaction program", the user at his remote personal computer terminal which will be, of course, equipped with a CD-ROM reader, will load the CD-ROM disk into his computer and log onto an access program or user program (which may optionally be recorded on the CD-ROM disk as well). The user program then transmits the user's individual access key code (which optionally may be encrypted) over a communication network or over a telephone network to the host computer or server, which will be appropriately programmed to check the user's access key code against the registry of stored authorized individual user access key codes. The server program will further include the requisite steps to interdict and end any attempt to gain access to the server or transaction program through a transmitted access code which is not stored in the database of authorized individual user access key codes. The server program will disconnect and may optionally inform the user that an unauthorized key access code has been transmitted.

Alternatively, and assuming the CD-ROM disk was proper and contained an authorized access key code, the communication between the user's remote computer and the host server will continue with the host computer's program including steps to grant access to the user's program and begin the session. As will be explained hereinafter, the host computer program or server program and the user program may optionally encrypt the session using the user's encryption key or keys, which are also stored in the server's database and on the individual user's CD-ROM disk. The optional encryption might also include encryption keys which are stored on the user's CD-ROM disk key.

At this stage, access to the secured database or "secured server transaction program" can proceed with the authorized user communicating through his own personal computer with the host server to conduct whatever "transaction" he may wish to effect, ranging from the simple ordering of merchandise, to the conduct of financial transactions, to conduct of research into a secured database, or any other type of two-way communication which is capable of being conducted between a remote computer terminal and a host terminal over a communication network or a telephone network. It is to be understood that a level of security heretofore unavailable to remote consumers communicating with a host computer is provided by the new system which utilizes ultra long identification key codes typically impressed upon or otherwise recorded upon "large keys" in the form of a CD-ROM disk or the like. The ultra long identification keys are checked and approved through databases of such identification keys which are stored in a remote host computer or server.

Note that in some applications, the key generation algorithm might run on the server itself or even on the users'

computers; in the latter case, means to avoid generating duplicate keys would be required (e.g. by a randomization function in the key generation algorithm, plus a check for duplicate keys whenever a new key is added to the database). The block diagram of FIG. 1 would then be modified accordingly.

Numerous other variants will also readily be apparent to those skilled in the art.

In a preferred embodiment, each user is issued a unique CD-ROM disk containing one or more unique identification keys. An individual user inserts his CD-ROM disk "key" into a computer connected via a network or other communications device to a host computer; also referred to herein as a server. An access program on the CD-ROM "key" connects to and forwards the unique identification key from the CD-ROM disk key to the host computer in encrypted form. A security authentication program stored on the server then decrypts the identification key, compares the identification key with an identification key from the database of user identification keys located on a large capacity storage device connected to the host computer, and verifies the user's identity. The host computer may include a program which will also demand that the user type in a password. If the identification key matches the identification key in the host computer's database of user identification keys and if the user enters the correct password, the host computer, through its programming, will grant access to the user.

The host computer (server) will be further programmed to require the remotely accessed terminal program to re-authenticate itself at regular intervals. This helps defend against thieves who capture an identification key en route to the host computer or who misappropriate or steal a user's connection. Unless a thief has the unique CD-ROM "key", he would be unable to use his unauthorized access for longer than the time between requested re-authentications.

Although individual identification keys are contemplated, in some applications, some or all of these identification keys may be shared among a class or subclass of users.

In another embodiment, the host computer is programmed to send an encryption key to the remote terminal. The terminal program executing on the remote terminal uses the encryption key to encrypt the unique identification key on the CD-ROM disk. Then the encrypted identification key is sent to the host computer for verification. If the encryption means is a public key encryption algorithm with a sufficiently long key, a third party would have great difficulty extracting the unencrypted identification. A variation to this method is to have part of the encryption key contained on the user's CD-ROM "key" with the other part sent from the host computer. The host computer always has access to a complete database of all the encryption keys and identification keys. Without the portion of the encryption key from the CD-ROM or host computer, the remote terminal program is unable to decrypt messages. If the encryption key from the host computer is varied with time, selected randomly, or unique to each user session, the user's computer will essentially never transmit the same encrypted identification key twice.

The remote terminal program can pad the identification key with random, null, or nonsense prefixes or suffixes or interpolated characters. To insure that the same identification message is not sent twice, the encryption algorithm is provided with good diffusion (wherein a change in any character in the plain text changes many or all of the characters in the encrypted text). The pad will preferably be specified by the host computer so that previously used encrypted identification keys do not repeat.